

CLAIMS

[0056] What is claimed is:

1. A method comprising:

selecting, based on a predetermined criterion related to a successful transmission of a data packet, one of at least first and second protection mechanisms to protect said data packet.
2. The method of claim 1, wherein selecting comprises selecting to modulate said data packet using a first modulation type and to protect said data packet using said first protection mechanism, to modulate said data packet using said first modulation type and to protect said data packet using said second protection mechanism, or to modulate said data packet using a second modulation type.
3. The method of claim 2, wherein said first modulation type comprises orthogonal frequency division multiplexing, and wherein said second modulation type comprises direct sequence spread spectrum/complementary code keying.
4. The method of claim 1, wherein said first protection mechanism comprises a request-to-send/clear-to-send protection mechanism, and wherein said second protection mechanism comprises a clear-to-send-to-self protection mechanism.
5. The method of claim 1 comprising estimating at least one of a first parameter related to said data packet being protected using said first protection mechanism, a second parameter related to said data packet being protected using said second protection mechanism, and a third parameter related to said data packet not being protected, wherein said criterion relates to one or more of said parameters.
6. The method of claim 5, wherein at least one of said parameters is a time period for successful transmission of said data packet.
7. The method of claim 5, wherein at least one of said parameters is a power consumption for successful transmission of said data packet.
8. The method of claim 5, wherein estimating comprises estimating at least one of said parameters based on one or more of a length of said data packet, a collision probability, a rate of a first modulation type, and a rate of a second modulation type.

9. The method of claim 5, wherein selecting based on said predetermined criterion comprises comparing between at least two of said first, second and third parameters.
10. The method of claim 5 comprising:
- selecting to protect said data packet using said first protection mechanism if said third parameter is greater than said second parameter and said first parameter is smaller than said second parameter; and
 - selecting to protect said data packet using said second protection mechanism if said first and third parameters are greater than said second parameter.
11. The method of claim 5 comprising selecting not to protect said data packet if said third parameter is smaller than said first and second parameters.
12. An apparatus comprising a controller able to select, based on a predetermined criterion related to a successful transmission of a data packet, one of at least first and second protection mechanisms to protect said data packet.
13. The apparatus of claim 12, wherein said controller is able to select to modulate said data packet using a first modulation type and to protect said data packet using said first protection mechanism, to modulate said data packet using said first modulation type and to protect said data packet using said second protection mechanism, or to modulate said data packet using a second modulation type.
14. The apparatus of claim 13, wherein said first modulation type comprises orthogonal frequency division multiplexing, and wherein said second modulation type comprises direct sequence spread spectrum/complementary code keying.
15. The apparatus of claim 12, wherein said first protection mechanism comprises a request-to-send/clear-to-send protection mechanism, and wherein said second protection mechanism comprises a clear-to-send-to-self protection mechanism.
16. The apparatus of claim 12, wherein said controller is able to estimate at least one of a first parameter related to said data packet being protected using said first protection mechanism, a second parameter related to said data packet being protected using said second protection mechanism, and a third parameter related to said data packet not being protected, wherein said criterion relates to one or more of said parameters.

17. The apparatus of claim 16, wherein said controller is able to estimate at least one of said parameters based on one or more of a length of said data packet, a collision probability, a rate of a first modulation type, and a rate of a second modulation type.
18. The apparatus of claim 16, wherein at least one of said parameters is a time period for successful transmission of said data packet.
19. The apparatus of claim 16, wherein at least one of said parameters is a power consumption for successful transmission of said data packet.
20. The apparatus of claim 16 wherein said controller is able to compare between at least two of said first, second and third parameters.
21. The apparatus of claim 16, wherein said controller is able to:
 - select to protect said data packet using said first protection mechanism if said third parameter is greater than said second parameter and said first parameter is smaller than said second parameter; and
 - select to protect said data packet using said second protection mechanism if said first and third parameters are greater than said second parameter.
22. A wireless device comprising:
 - a controller able to select, based on a predetermined criterion related to a successful transmission of a data packet, one of at least first and second protection mechanisms to protect said data packet; and
 - one or more omni-directional antennas able to transmit said data packet.
23. The wireless device of claim 22, wherein said controller is able to select to modulate said data packet using a first modulation type and to protect said data packet using said first protection mechanism, to modulate said data packet using said first modulation type and to protect said data packet using said second protection mechanism, or to modulate said data packet using a second modulation type.

24. The wireless device of claim 22, wherein said first protection mechanism comprises a request-to-send/clear-to-send protection mechanism, and wherein said second protection mechanism comprises a clear-to send-to-self protection mechanism.

25. The wireless device of claim 22, wherein said controller is able to estimate at least one of a first parameter related to said data packet being protected using said first protection mechanism, a second parameter related to said data packet being protected using said second protection mechanism, and a third parameter related to said data packet not being protected, wherein said criterion relates to one or more of said parameters.

26. The wireless device of claim 25, wherein said controller is able to compare between at least two of said first, second and third parameters.

27. The wireless device of claim 25, wherein at least one of said parameters is a time period for successful transmission of said data packet.

28. The wireless device of claim 25, wherein at least one of said parameters is a power consumption for successful transmission of said data packet.

29. A system comprising:

a first communication device comprising:

a controller able to select, based on a predetermined criterion related to a successful transmission of a data packet, one of at least first and second protection mechanisms to protect said data packet; and

one or more antennas able to transmit said data packet; and

a second communication device able to receive one or more data packets transmitted by said first device.

30. The system of claim 29, wherein said controller is able to estimate at least one of a first parameter related to said data packet being protected using said first protection mechanism, a second parameter related to said data packet being protected using said second protection mechanism, and a third parameter related to said data packet not being protected, wherein said criterion relates to one or more of said parameters.

31. The system of claim 30, wherein at least one of said parameters is a time period for successful transmission of said data packet.

32. A program storage device having instructions readable by a machine that when executed by the machine result in:

selecting, based on a predetermined criterion related to a successful transmission of a data packet, one of at least first and second protection mechanisms to protect said data packet.

33. The program storage device of claim 32, wherein the instructions resulting in selecting result in selecting to modulate said data packet using a first modulation type and to protect said data packet using said first protection mechanism, to modulate said data packet using said first modulation type and to protect said data packet using said second protection mechanism, or to modulate said data packet using a second modulation type.

34. The program storage device of claim 32, wherein said instructions result in estimating at least one of a first parameter related to said data packet being protected using said first protection mechanism, a second parameter related to said data packet being protected using said second protection mechanism, and a third parameter related to said data packet not being protected, wherein said criterion relates to one or more of said parameters.

35. The program storage device of claim 34, wherein the instructions resulting in selecting based on said predetermined criterion result in comparing between at least two of said first, second and third parameters.